Remarks

Upon entry of the foregoing amendment, claims 2, 3, 28-30, 32-36, and 44-46 are pending in the application, with claim 46 being the independent claims. Claims 32, 33, and 46 are sought to be amended. These changes are believed to introduce no new matter, and their entry is respectfully requested.

Based on the above amendment and the following remarks, Applicant respectfully requests that the Examiner reconsider all outstanding objections and rejections and that they be withdrawn.

Objections to the Claims

Claims 32 and 33 were objected to because of informalities. Applicant has amended claims 32 and 33 as suggested by the Examiner. Reconsideration and withdrawal of the rejection are therefore respectfully requested.

Rejections under 35 U.S.C. § 112

Claims 2, 3, 28-30, 32-26, and 44-46 were rejected under 35 U.S.C. § 112, first paragraph, as failing to comply with the written description requirement. Specifically, the Office Action states that it is "unclear where 'any remaining payload data' is found within these tables (or elsewhere in the current specification or provisional application 60/235,190), since it appears as though crypto processing on the payload is performed separately from crypto processing on the MAC or hash created from the header." (Office Action, p. 4).

Table 1: SSL Outbound shows the order of events that transpire during an SSL outbound session. As shown in Table 1, cryptographic processing occurs in SSL_Ob_6, SSL_Ob_8, and SSL_Ob_A. For example, in SSL_Ob_4, the front end

(fe) sends payload data to the authentication input FIFO (AIF) and the Cryptographic input FIFO (CIF). The authentication unit processes the MAC in SSL_Ob_5 and the cryptographic unit processes a portion of the payload data in SSL_Ob_6.

The generated authentication code (MAC) is fed back to the alignment logic (as shown in FIG. 3). The next set of data is then processed by the cryptographic unit in SSL_Ob_8. The alignment unit pads the MAC and any remaining payload data in SSL_Ob_9 (see also FIG. 5 of the current specification) and the cryptographic unit processes the remainder of the data.

As described in paragraphs [0032] and [0033] of the specification, the payload data is processed by the DES engine in 64-bit blocks. Therefore, if the payload is greater than 64-bits in length, payload will remain in the FIFO after the first 64-bit block is being processed by the DES engine. Therefore, both Table 1 and the current specification describe "performing encryption operations on any remaining payload data for the first packet and the authentication code for the first packet," as recited in previously presented independent claim 46.

For at least these reasons, independent claim 46 complies with the written description requirement. Accordingly, its dependent claims 2, 3, 28-30, 32-36, 44, and 45 also comply with the written description requirement. Reconsideration and withdrawal of the rejection are therefore respectfully requested.

Rejections under 35 U.S.C. § 103

Kaplan, Larsen, and Huynh

Claims 28-30, 33, 35, 36, and 44-46 were rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,704,871 to Kaplan ("Kaplan") in view of

U.S. Patent No. 7,068,791 to Larsen ("Larsen") and U.S. Patent No. 6,983,366 to Huynh ("Huynh"). Applicant respectfully traverses this rejection.

The combination of Kaplan, Larsen, and Huynh does not teach or suggest each and every element of amended independent claim 46. Kaplan describes that "the same input data stream is internally buffered by both the hash and encryption sections, depending on the data flow of the operation selected. In the case of hash-encrypt, ... the two components of the operation are done in parallel." (Kaplan, col. 42, lines 48-50). The hash-encrypt command is used "to perform a hash calculation and symmetrical encryption of the customer's data." (Kaplan, col. 168, lines 60-62). As illustrated in FIG. 9, the output of the Hash Block is fed into the context storage block (O/I). (Kaplan, FIG. 9). The context information is then fed into the encrypt/decrypt block. As further illustrated in Kaplan, the pad insertion occurs prior to any encryption (and receipt of authentication code). (Kaplan, FIG. 9).

Thus, Kaplan does not teach or suggest:

> performing encryption operations on a set of data in the payload data for the first packet, wherein the encryption operations on the set of payload data for the first packet is performed in parallel with the authentication operations for the first packet;
>
> . . .
>
> adding padding to the remaining payload data for the first packet and the authentication code for the first packet to generate a data block having a predefined length;
>
> performing encryption operations on the remaining payload data for the first packet, the authentication code for the first packet, and the padding;

as recited in amended independent claim 46. Neither Larsen nor Huynh overcome these deficiencies of Kaplan. Claims 28-30, 33, 35, 36, 44, and 45 depend from claim

46. For at least the above reasons, and further in view of their own features, dependent claims 28-30, 33, 35, 36, 44, and 45 are patentable over the combination of Kaplan, Larsen, and Huynh. Reconsideration and withdrawal of the rejection are therefore respectfully requested.

Kaplan, Larsen, Huynh, and SSL3spec

In the Office Action, claim 2 was rejection under 35 U.S.C. §103(a) as being unpatentable over Kaplan, Larsen, Huynh in view of Freier, et al, "The SSL Protocol Version 3.0," November 18, 1996, pp. 1-12 (SSL3spec). Applicant respectfully traverses this rejection.

Claim 2 depends from independent claim 46. The SSL3spec does not overcome the deficiencies of Kaplan, Larsen, and Huynh described above relative to claim 46. For at least these reasons, and further in view of its own features, claim 2 is patentable over the combination of Kaplan, Larsen, Huynh, and SSL3spec. Reconsideration and withdrawal of the rejection is therefore respectfully requested.

Kaplan, Larsen, Huynh, and TLSspec

In the Office Action, claim 3 was rejected under 35 U.S.C. §103(a) as being unpatentable over Kaplan, Larsen, Huynh in view of Dierks, et al, "The TLS Protocol Version 1.0" (TLSspec). Applicant respectfully traverses this rejection.

Claim 3 depends from claim 46. The TLSspec does not overcome the deficiencies of Kaplan, Larsen, and Huynh described above relative to claim 46. For at least these reasons, and further in view of its own features, claim 3 is patentable over the combination of Kaplan, Larsen, Huynh and TLSspec. Reconsideration and withdrawal of the rejection is therefore respectfully requested.

Kaplan, Larsen, Huynh and Ganapathy

In the Office Action, claim 32 was rejected under 35 U.S.C. §103(a) as being unpatentable over Kaplan, Larsen, Huynh, further in view of Ganapathy, U.S. Patent 6,557,096 (Ganapathy). Applicant respectfully traverses this rejection.

Claim 32 depends from claim 46. Ganapathy does not overcome all the deficiencies of the combination of Kaplan, Larsen, and Huynh relative to independent claim 46 described above. For at least these reasons and further in view of its own features, claim 32 is patentable over the combination of Kaplan, Larsen, Huynh and Ganapathy. Reconsideration and withdrawal of the rejection is therefore respectfully requested.

Kaplan, Larsen, Huynh and Gaytan

In the Office Action, claim 34 was rejected under 35 U.S.C. §103(a) as being unpatentable over Kaplan, Larsen, Huynh in view of Gaytan, U.S. Patent 5,638,367 (Gaytan). Applicant respectfully traverses this rejection.

Claim 34 depends from claim 46. Gaytan does not overcome all the deficiencies of Kaplan, Larsen, and Huynh relative to independent claim 46 described above. For at least these reasons and further in view of its own features, claim 34 is patentable over the combination of Kaplan, Larsen, Huynh and Gaytan. Reconsideration and withdrawal of the rejection is therefore respectfully requested.

Conclusion

All of the stated grounds of objection and rejection have been properly traversed, accommodated, or rendered moot. Applicant therefore respectfully

requests that the Examiner reconsider all presently outstanding objections and rejections and that they be withdrawn. Applicant believes that a full and complete reply has been made to the outstanding Office Action and, as such, the present application is in condition for allowance. If the Examiner believes, for any reason, that personal communication will expedite prosecution of this application, the Examiner is invited to telephone the undersigned at the number provided.

Prompt and favorable consideration of this Amendment and Reply is respectfully requested.

Respectfully submitted,

STERNE, KESSLER, GOLDSTEIN & FOX P.L.L.C.

Lori A. Gordon
Attorney for Applicant
Registration No. 50,633

Date: August 25, 2008

1100 New York Avenue, N.W.
Washington, D.C. 20005-3934
(202) 371-2600

804582_1.DOC